Claims

1. Method of securing access to a piece of equipment (EQP), this method comprising at least: one attribution operation consisting of supplying a reference datum (CRYPT_SGN02) to an authentication medium (CRD); an acquisition operation consisting of obtaining, for every access request formulated by a party requesting access to the equipment, a biometric signature (SGN) of this party requesting access; and a verification step consisting of verifying, by means of the reference datum (CRYPT_SGN02), the authenticity of the biometric signature (SGN) obtained from the party requesting access, characterised in that it comprises a prior encryption step, during which an encrypted version (CRYPT_SGN02) of at least one authentic biometric signature (SGN02) belonging to at least one person authorised to access the piece of equipment is created, in that the verification step comprises a decryption operation implemented in the authentication medium (CRD) and consisting of decrypting, by means of a secret key (K, K0), the encrypted version (CRYPT_SGN02) of an authentic biometric signature (SGN02) supplied to this authentication medium (CRD) as a reference datum during the access request, and in that the verification step comprises a comparing operation implemented by secretly comparing the biometric signature (SGN) obtained from the party requesting access during the access request with the

authentic biometric signature (SGN02) that results from the decryption step.

2. Authentication medium for implementing the method according to claim 1, characterised in that it is in the form of an electronic card comprising at least one decryption module (DECRYPT) using a secret key (K, K0).

3. Authentication medium according to claim 2, characterised in that it also comprises a comparison module (COMPAR).

4. Authentication medium according to claim 2 or 3, characterised in that it also comprises an encryption module (ENCRYPT).

5. Device for securing access to a piece of equipment, this device comprising: an authentication medium (CRD) which is supplied with a reference datum (CRYPT_SGN02); a sensor (CAPT) obtaining, during every access request formulated by a party requesting access to the equipment, a biometric signature (SGN) of this party requesting access; and control means (CTRL) included in the authentication medium (CRD) and selectively authorising the party requesting access to access the piece of equipment (EQP) in accordance with the result of a verification of the authenticity of the biometric signature of the party requesting access by means of the reference datum (CRYPT_SGN02), characterised in that the control means (CTRL) comprise a decryption module (DECRYPT) and a comparison module (COMPAR), in that the reference datum (CRYPT_SGN02) supplied to the authentication medium (CRD) consists of

an encrypted version of an authentic biometric signature (SGN02) allegedly attributed to the party requesting access, in that the decryption module (DECRYPT) uses a secret key (K, K0) by means of which it secretly reconstructs, upon each access request, the authentic biometric signature (SGN02) from its encrypted version (CRYPT_SGN02), and in that the comparison module (COMPAR) secretly compares the biometric signature (SGN) obtained from the party requesting access with the reconstructed authentic biometric signature (SGN02), and supplies a comparison result (RESULT) that constitutes the result of the verification.

6. Security device according to claim 5, characterised in that the authentication medium (CRD) is a card, removable or non-removable, equipped with a memory that cannot be read from outside, in which the secret key (K, K0) is stored.

7. Security device according to either one of the claims 5 or 6, characterised in that it comprises at least one computer (ORDI) that makes up at least a part of the equipment (EQP) to which the access is secured.

8. Security device according to claim 7, characterised in that the computer (ORDI) contains in its memory a plurality of personal identification codes (PIN1, PIN2, PIN3) attributed to a corresponding plurality of persons authorised to access the equipment and associated with a corresponding plurality of encrypted authentic biometric signatures (CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03) for these authorised persons,

and in that the computer (ORDI) delivers to the identification medium (CRD), when receiving an access request, the encrypted authentic biometric signature (CRYPT_SGN02) that corresponds to the identification code (PIN2) supplied by the party requesting access, which means that a single authentication medium (CRD) provides several persons with secure access to the computer (ORDI).

9. Security device according to any one of the claims from 5 to 8, characterised in that it comprises an encryption module 5 to 8, characterised in that is comprises an encryption module (ENCRYPT, ENCRYPT_K1) that is able to delivering an encrypted version of an authentic biometric signature supplied in plain form by the sensor (CAPT) in response to an encryption command.

10. Security device according to claim 9, characterised in that the secret key (K0) is a private key with a matching public key (K1), and in that the encryption module (ENCRYPT_K1) is included in the computer (ORDI) and uses the public key (K1).